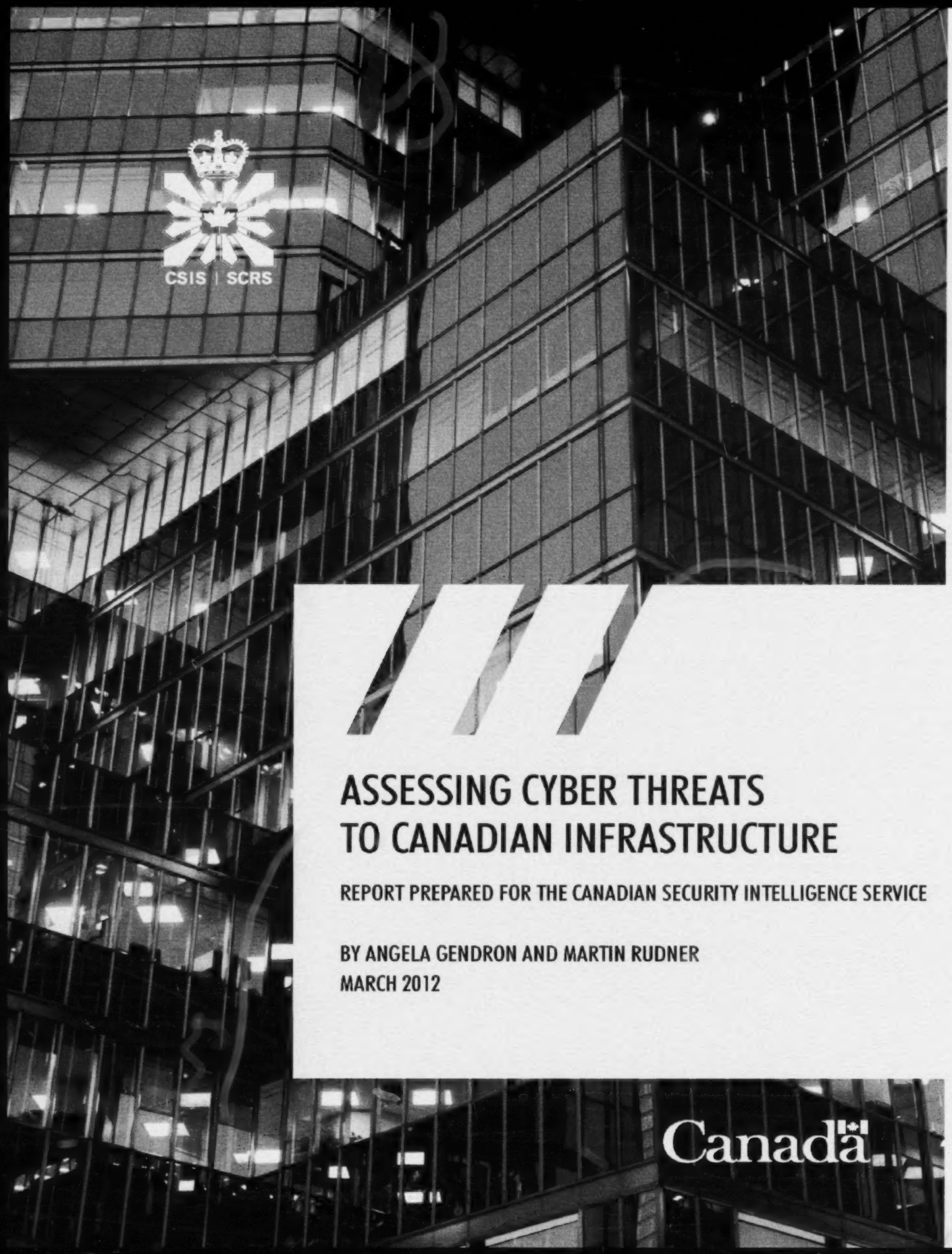

ASSESSING CYBER THREATS TO CANADIAN INFRASTRUCTURE

REPORT PREPARED FOR THE CANADIAN SECURITY INTELLIGENCE SERVICE

BY ANGELA GENDRON AND MARTIN RUDNER

MARCH 2012

Canada

Think recycling

This document is printed with environmentally friendly ink

Occasional Papers 2012-10-01

This Study was commissioned by the Canadian Security Intelligence Service (CSIS). The views expressed are those of the author and do not reflect any official position of CSIS.

Photo credit: istockphoto.com

ASSESSING CYBER THREATS TO CANADIAN INFRASTRUCTURE

REPORT PREPARED FOR THE CANADIAN SECURITY INTELLIGENCE SERVICE

BY ANGELA GENDRON AND MARTIN RUDNER

MARCH 2012

TABLE OF CONTENTS

EXECUTIVE SUMMARY 5

CHAPTER 1 - CANADIAN INFRASTRUCTURE AND INTERDEPENDENCIES 11

Background 11
Structural Dynamics of Canada's Critical 14
Infrastructure Sectors
Energy and Utilities 14
Transportation 15
Finance 16
Information and Communications Technology 16
Infrastructure and Interdependencies 17

CHAPTER 2 - THE CYBER-THREAT ENVIRONMENT 21

International Terrorism 22
State Sponsored Terrorism, Espionage and Sabotage 26
Malicious Hacktivism 30
Insider Threats 34

CHAPTER 3 - RISKS AND PROBABILITIES OF CYBER-ATTACKS 37

The Cyber Domain: Characteristics and Concerns 37
Emergent Threats 40
Assessing Risks and Vulnerabilities 42

CHAPTER 4 COUNTERING THE CYBER-THREATS: A PARTNERSHIP APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION 43

A WAY AHEAD 43

APPENDIX A 49
THE STRUCTURAL DYNAMICS OF THE INFORMATION AND COMMUNICATIONS TECHNOLOGY SECTOR

APPENDIX B 53
MODELING RISKS AND VULNERABILITIES

ENDNOTES 55

ASSESSING CYBER THREATS TO CANADIAN INFRASTRUCTURE

EXECUTIVE SUMMARY

The purpose of this study is threefold: (1) to examine the cyber threat environment confronting Canada's Critical National Infrastructure (CNI), with a particular focus on four key sectors and their inter-dependencies, namely Energy and Utilities, Transportation, Finance, and Information and Communications Technology; (2) to identify those entities with the capability and political/ideological motivation to launch cyber attacks against this country's CNI and pose a threat to our national interests; and (3) to discuss the role of intelligence in countering these threats. The cyber activities of criminals and organized crime gangs that are motivated by financial or material gain are excluded from this study.

BACKGROUND

Threats to critical infrastructure were identified as a national security priority concern in Canada's National Security Policy, *Securing an Open Society* (2004). Subsequently, the *National Strategy for Critical Infrastructure* (2010) categorized critical infrastructure into sectors that all have in common a computerized element upon which physical systems are dependent. Increasingly, these sectors have become more interconnected and interdependent, which renders them more vulnerable to cyber threats and makes them a more attractive target. A cyber attack could potentially cause widespread damage to digital networks as well as physical disruption and destruction.

Primary responsibility for protecting critical assets rests with the owner-operators. However, given the interdependencies within and across infrastructure sectors and jurisdictions, successfully countering the threats, mitigating consequences and improving resilience can only be achieved by a public/private sector partnership that engages all stakeholders. National-level information-sharing networks that are sector-specific have now been established.

In October 2010, the government's *Cyber Security Strategy* called for a comprehensive assessment of the threats, vulnerabilities and risks to Canada's Critical Infrastructure arising from cyber attacks. A recently issued counter-terrorism strategy, *Building Resilience Against Terrorism*, acknowledges that terrorists have "shown an interest" in developing cyber capabilities for attacks against critical infrastructure, and proposes a proactive approach to deny terrorists "the means and opportunities to act in Canada." It further states that a strong intelligence capacity is required in order to understand the strategic drivers of the threat environment and detect potential terrorists and their activities.

STRUCTURAL DYNAMICS OF CANADA'S CRITICAL INFRASTRUCTURE SECTORS

The defining feature of a modern, knowledge-based society and its economy is their dependence on information and communications technologies (ICT). The four sectors that are the focus of this report operate in a globally competitive economic environment in which such technologies are increasingly being used to promote efficiencies and operational effectiveness. The products and services of each of these sectors are important to the well-being and prosperity of Canadians as well as being significant contributors to Canada's GDP. Furthermore, Canada's energy sector is closely integrated with the United States at a continental level, so that any major supply disruptions would have a profound effect not only on Canadian consumers but also on export markets in the United States.

New technologies include computerized control systems that are used by many industries and critical national infrastructures to monitor and control sensitive processes and physical functions. This growth in connectivity, coupled to the inherent insecurity of Internet connections, has escalated the risks of cyber attacks.

INFRASTRUCTURE AND INTERDEPENDENCIES

Interdependencies exist when producers and suppliers of products and services both ***within*** and ***between*** critical infrastructure sectors become mutually dependent upon one another, albeit to varying and unequal degrees. In the past, dependence stemmed from physical or geographic relationships. The development of cyberspace has led to the creation of additional relationships, which create further vulnerabilities.

Internet-linked data communications systems and computerized methods of automatic command and control by remote electronic means are widespread across Canadian critical infrastructure. They enable central monitoring and control over production and delivery processes at particular facilities and interdependent infrastructures across wide geographic areas. Increasing connectivity means that the failure of one critical component is liable to have far-reaching, reverberating effects. Disruptions in the availability of products and services can have serious commercial and societal consequences that cascade not only across sectors but also across jurisdictions—private/public, provincial, territorial and federal.

The complexity of these links means that achieving a sufficiently comprehensive "situational awareness" is a major challenge for owner/operators. Reducing the risks arising from interdependencies requires a collaborative private/public sector approach.

THE CYBER-THREAT ENVIRONMENT

The cyber dimension has transformed key economic infrastructure and national assets into more attractive, high-value targets, while at the same time rendering them more vulnerable to significant threats. In an asymmetric environment, cyberspace provides a relatively low-cost, risk-free haven for a broad range of disruptive and intelligence-gathering operations.

The major threats arise from international terrorism (which may be encouraged and assisted by foreign interference or state entities); state-sponsored espionage and sabotage; and malevolent hacktivism. Any of these possibilities may involve the use of an 'insider' to carry out or assist in the attack. In its early stages, it may not be possible to specify whether a cyber incident is state-sponsored, autonomous or perpetrated by a malicious or criminal group.

a) International terrorism, specifically Sunni Islamist extremism, has been identified in the new Counter-terrorism Strategy as the leading threat to Canada's national security. Although the Energy, Transport and Finance sectors have long been attractive targets in terms of physical attacks, there is now growing concern that Islamists will use the Internet to launch cyber attacks to promote their so-called economic jihad. As yet, there is no evidence of systematic cyber-terrorism on the part of al-Qaeda or its affiliates, but al-Qaeda

has called explicitly for a cyber jihad alongside other terror operations, while certain Islamic scholars have affirmed the religious legitimacy of "electronic jihad."

b) State-sponsored terrorism, espionage and sabotage are also a source of concern: To the extent that terrorist individuals and groups attract state-sponsors, the threat to computer networks may rise. Advanced Persistent Threats (APTs), the most significant computer infections developed so far, require levels of technical and financial resources that have been associated with states.

Canada's dependence on digital networks and Internet-based communications, its open society and the attractiveness of its advanced industries as targets for intellectual property theft leave it vulnerable to cyber-espionage and sabotage activities. Many of these cyber attacks are reportedly attributed to government-backed hackers from China and Russia. The cyber dimension has changed the character of espionage in that non-state actors and the use of cyber cut-outs and technologies make detection and attribution difficult.

c) Most hacking incidents are motivated by criminality, protest or technical challenge. However, malicious hacking by activists, or hacktivists, who target the computer-controlled operating systems of critical infrastructure, constitutes a potential threat to national security. Major supply disruptions or exposure of sensitive government files may lead to widespread human suffering, if not loss of life, and loss of confidence in government.

d) New cyber technologies relating to the aggregation, storage and retrieval of data have contributed to the growing threat from insiders. Whether aggrieved, suborned or infiltrated, insiders engaging in activities within high-tech manufacturing and resource industries, energy utilities, and government departments and agencies have become a cause of significant concern. The U.S. Department of Homeland Security (DHS) has warned that violent extremists have obtained insider positions in American energy utilities and present a significant physical and cyber threat to critical infrastructure.

RISKS AND PROBABILITIES OF CYBER ATTACKS

Rapidly evolving techniques and technologies have given rise to new and more sophisticated threats based on the improvement of attackers' skill sets and the advanced technology at their disposal. At the same time, outsourcing the design, implementation and maintenance of ICT across all sectors to third-party providers, including developing countries, cloud computing and large data fusion centres, along with the use of off-the-shelf commercial technologies, has increased vulnerabilities and risks.

The speed of evolving new cyber threats, the lack of geographic boundaries and the problem of determining attribution impede efforts to counter attacks on information systems. Obstacles include not only domestic jurisdictional barriers to effective regulation, legislation and information-sharing but also the fragmented ownership and regulatory control of ICT infrastructure, which represents a major challenge at the global level.

A reliable method of estimating risk to critical infrastructure would help managers decide how much security is needed at a particular facility, but structural complexity and informational impediments hamper efforts to produce realistic assessments of threats and vulnerabilities. Some of the latest risk analysis methodologies attempt to integrate "wicked risks" (those, like terrorism, that cannot be determined through conventional actuarial methods) into their probability assessments.

COUNTERING THE THREATS: A PARTNERSHIP APPROACH TO INFRASTRUCTURE PROTECTION

Existing defensive measures will not suffice to ensure the integrity and availability of Canadian information systems or to prevent critical infrastructure from being disrupted or damaged. If information security is viewed as a purely technical problem, efforts to improve it will produce engineering solutions, mostly from the private sector. A more holistic, national-level strategy, however, might consider the issue in terms of *protecting an information-based society as a whole*, rather than protecting information infrastructures. This approach requires intelligence services to adopt a proactive cyber-security initiative focused on *preventing* infections rather than merely reacting to them. It would also place

greater emphasis on combating cyber exploitations that target government and business secrets—which are as much a threat to national security as large cyber attacks intended to damage or disrupt computer systems.

Owner/operators of critical infrastructure have primary responsibility for the protection of their assets, but national security is the prerogative of the state; securing critical assets against cyber threats that have ramifications for national security requires a partnership of all stakeholders, who may also need to consider how the financial costs of securing critical infrastructure will be shared by all those who benefit.

THE WAY AHEAD

Intelligence is a key component of tactical and strategic decision-making. In the cyber domain, intelligence can enhance the ability of governments and stakeholders to detect threats, assess the cyber capabilities of adversaries, evaluate the effects of cyber attacks, mitigate the risks, and streamline cyber security into an efficient and cost-effective process based on well-informed decisions. The aim must be to ensure that the cost to adversaries of trying to exploit systemic vulnerabilities is high; that the prospects of success are minimal; and that industry and society are properly prepared for resilience.

Canada's new counter-terrorism strategy explicitly supports proactive intelligence and law enforcement actions to make Canada a more difficult target for terrorists. Countering cyber threats to critical infrastructure requires an approach that goes beyond defensive, technical solutions and applies Canada's intelligence capabilities and assets (including signals intelligence) to the challenge of identifying and preventing prospective attacks.

ASSESSING CYBER THREATS TO CANADIAN INFRASTRUCTURE

CHAPTER 1
CANADIAN INFRASTRUCTURE AND INTERDEPENDENCIES

This study examines the cyber-threat environment confronting Canada's Critical National Infrastructure (CNI), with a particular focus on four key sectors and their interdependencies, namely Energy and Utilities, Transportation, Finance, and Information and Communications Technology. It identifies those entities with the capability and political/ideological motivation to launch cyber attacks against this country's CNI and poses a threat to our national interests. Lastly, it discusses the role of intelligence in countering these threats. The cyber activities of criminals and organized crime gangs that are motivated by financial or material gain are excluded from this study.

BACKGROUND

Most critical infrastructures share three characteristics: their symbolic importance or power; the degree and immediacy of dependence on the infrastructure for the functioning of a society; and the known and unanticipated effects of complex dependencies that have consequences beyond the local. Different countries have different definitions of criticality, but what they all have in common is the existence of a computerized element upon which physical systems are dependent and which, if harmed, would likely cause widespread damage in physical terms.[1]

The nexus between cyber and critical infrastructure was already recognized by the turn of the millennium, as Canada (along with other jurisdictions) faced the so-called Y2K challenge, which in turn led to the creation of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). The term "cyber attack" is commonly used to describe a range of cyber incidents that are launched with different intent by various actors—individuals, organized and loosely affiliated groups, and states.[2]

Threats to critical infrastructure were first identified as a national security priority concern by Canada's National Security Policy, *Securing an Open Society* (2004).[3] Subsequently, the *National Strategy for Critical Infrastructure,*[4] released in May 2010, identified ten critical infrastructure sectors and placed their protection under the stewardship of their respective federal government departments or agencies. Overall leadership for promoting the resilience of crucial infrastructure was assigned to Public Safety Canada. Sectoral responsibility for critical infrastructure is allocated as follows:

- Energy and Utilities: Natural Resources Canada
- Information and Communications Technology: Industry Canada
- Finance: Finance Canada
- Food: Agriculture and Agri-Food Canada
- Health: Public Health Agency of Canada
- Manufacturing: Industry Canada, Department of National Defence
- Safety: Public Safety Canada
- Transportation: Transport Canada
- Water: Environment Canada

The National Strategy for Critical Infrastructure adopted an all-hazards approach, and recognized that not only do interdependencies exist within and across critical infrastructure sectors, but also that these are further intensified by the increasing reliance on information and communication technologies (ICT). The Strategy was accompanied by an Action Plan that emphasized the building of partnerships involving other levels of government, the private sector and other stakeholders, while acknowledging that the primary responsibility for protecting their assets rests with owner-operators of critical infrastructure.[5]

As part of the partnership approach, sector networks have been established under the aegis of their respective line departments. Most of these sector networks are composed of owners and operators from the sector, mainly through their national industry associations, along with pertinent federal, provincial and territorial departments and agencies. Their role is to serve as national-level, sector-specific standing forums for addressing issues of shared concern regarding critical infrastructure protection, and to facilitate information-sharing and industry feedback. Because these sector networks are at different stages of maturity and experience, the resulting flow of information and vulnerability assessments across sectors and their interdependencies lacks consistency and coherence.

In addition, a National Cross-Sector Forum has been established to enable representatives of the sector networks and federal provincial and territorial governments to exchange information and also to address cross-sectoral interdependencies. This National Cross-Sector Forum has met annually since 2010.

Canada's Cyber-Security Strategy,[6] adopted in October 2010, outlined a course of action to engage with provinces, territories and the private sector in implementing a cyber-security strategy to protect the country's digital systems. This calls for a comprehensive assessment of the threats, vulnerabilities and risks to Canada's Critical Infrastructure arising from cyber attacks. The Cyber-Security Strategy aims to build on the partnership framework put in place under the National Strategy for Critical Infrastructure, especially in regard to private sector stakeholders.[7]

The Royal Canadian Mounted Police (RCMP) has established a Critical Infrastructure Intelligence Team to examine physical and cyber threats to critical infrastructure, whose tools include a Suspicious Incident Reporting system designed to gather information from private industry and local law enforcement about suspicious incidents.

Since fall 2011, the Canadian Cyber Incidence Response Centre (CCIRC) at Public Safety Canada has been re-positioned within its Emergency Management and National Security Branch as the designated entity for coordinating federal government responses to cyber security incidents of national interest and protecting critical infrastructure. CCIRC responsibilities include monitoring cyber threats, coordinating incident management and facilitating information-sharing for the protection of critical infrastructure.

In February 2012, Public Safety Canada introduced a Counter-terrorism Strategy entitled *Building Resilience Against Terrorism,* promulgating an integrated, layered approach to protecting Canadians and Canadian interests from terrorist attack. Its aim is to galvanize law enforcement efforts around clear strategic objectives.[8] The Strategy recognizes explicitly that terrorist groups have "expressed interest" in developing the capabilities for computer-based attacks against critical infrastructure.[9] The new Strategy, through its 'Deny' element, will pursue programs and activities aimed at reducing potential security vulnerabilities in the cyber domain, as well as in other areas of critical national infrastructure.[10]

STRUCTURAL DYNAMICS OF CANADA'S CRITICAL INFRASTRUCTURE SECTORS

Each of the four sectors addressed in this study has unique industrial or economic sub-sectors with their own distinctive structures, operating characteristics and vulnerabilities. Most are privately owned and operated. These various components of critical infrastructure operate in a globally competitive economic environment in which technological developments, especially in ICT, are an increasingly powerful driving force.

ENERGY AND UTILITIES

The Energy and Utilities sector encompasses oil and natural gas extraction and refining, pipelines, electricity generation and transmission, and nuclear power generation. In 2010 oil, gas and electricity production, processing and deliveries contributed about 6.2% of Canada's Gross Domestic Product. The Canadian energy industry possesses a high degree of criticality for the national, provincial and local economies, for consumers and user industries, and for public well-being in general. In recent years the energy sector has been operating at or near capacity, especially in electricity generation and oil refining, with little if any redundancy being readily available. Any sudden loss of capacity because of major damage to energy infrastructure would bring about immediate supply shortages, which in turn would cause prices to spike.

Canada's energy sector is closely integrated with the United States economy at a continental level through pipeline networks, electricity grids, and extensive commercial interactions among infrastructure owner/operators on both sides of the border. Canada has now become the single largest international supplier of oil and natural gas to the United States.

Oil industry leaders speaking at the World Petroleum Conference in Doha, Qatar, in December 2011, articulated their fears that cyber attacks on critical infrastructure could wreak havoc by destroying facilities or severely disrupting production and deliveries. Owing to interdependencies between energy and most other economic, social-sector and household requirements, any major disruption to the energy availability would inflict profound and far-reaching hardships on Canadians and on neighbouring export markets in the United States.

Over the past decade the structure of the electricity industry has undergone significant changes. The "unbundling" of the generation, transmission and distribution functions of electric utilities into separate organizations has increased the role of the private sector, while federal government investments in research and development have supported the commercialization of new technologies.

The electricity grids of Canada and the United States are closely interconnected and support wide-ranging interdependencies across their respective economies and societies. Future trends seem likely to open up new vulnerabilities in these grids by virtue of the introduction of advanced communications electronic devices from automated meters to synchrophasors. These technological advances risk creating new and additional vectors for cyber attackers to gain access to computer systems or other communicating equipment, thereby causing disruptions and even blackouts.

Overall responsibility for ensuring the reliability of the electric grid is vested in the North American Electric Reliability Council (NERC), an independent body that promotes the reliability and security of the bulk power system in the United States, Canada and parts of Mexico. NERC sets industry standards and monitors compliance, in addition to providing technical expertise on blackout investigation forensics and analysis. It requires operating companies to designate "critical cyber assets" and adopt appropriate physical and cyber security measures.

TRANSPORTATION

Canada's transportation infrastructure covers air transport, marine transport, railways, ports, urban transit, roadways, bridges and tunnels. The transportation sector plays a highly significant role in Canada's economy and society.

Future trends for urban transit include plans by Canada's Bombardier Inc. to introduce a fully integrated, contactless, electronic public-transport system called "Primove," which will use wireless technology for ongoing battery recharging, scheduling, ticketing, maintenance and other functions. This technology would drive a full range of electronic public-transportation vehicles sharing the same basic infrastructure.

FINANCE

Finance infrastructure includes banking, insurance, capital markets, credit/debit card facilities, and brokerage and financial services. Taken together, finance, insurance and real estate, along with the leasing and management of companies and enterprises, contributed approximately 20% of Canada's GDP in 2011, representing by far the largest segment of the Canadian economy.

Canadian banking and financial institutions are heavily dependent on IT and telecommunications systems for managing daily payments and clearing and settlement operations. Secure and resilient electricity supplies to these sectors are also vital. According to the Department of Finance, Canada's banks have over 8,000 branches and almost 18,000 automated teller machines (ATMs) across the country. Indeed, Canada has the highest number of ATMs per capita in the world as well as the highest utilization rate for electronic channels such as debit cards, Internet banking and telephone banking.

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

The ICT infrastructure sector includes telephony, radio and television broadcasting, internet connectivity, perimeter access controls, and space satellite monitoring and control. In a globally competitive environment, Canadian owner/operators of critical infrastructure facilities, like their counterparts elsewhere, are increasingly tending to introduce sophisticated cyber technologies in order to promote efficiencies and operational effectiveness.

These new technologies include computerized control systems that are used by many industries and critical national infrastructures to monitor and control sensitive processes and physical functions. Typically, Distributed Control Systems (DCS) are used within a single processing or generating plant or over a small geographic area, whereas Supervisory Control and Data Acquisition (SCADA) systems are used for large, geographically dispersed distribution operations. Such control systems perform vital functions across critical infrastructure sectors, including electric power generation, transmission and distribution; oil and gas refining and pipelines; water treatment and distribution; and railways and mass transit systems. However, the adoption of standardized technologies that have known vulnerabilities, increased connectivity of these control systems to others, insecure remote cyber connections and widespread

availability of technical information about control systems have escalated the risk of cyber attacks. The vulnerability of Internet communications poses significant risks to the critical infrastructures and operations they support.

ICT-based technologies are used in the transportation sector for air passenger reservations and boarding control and for air cargo management. They are also part of the Free and Secure Trade (FAST) and Pre-Arrival Processing System (PAPS) programs providing border pre-clearances for trucking. Internet-linked ICT systems are used in the Finance sector for operating client accounts (ATMs) and credit/debit card charge card devices, and for wire transfers of funds. (See Appendix A for further information on the structural dynamics of the ICT sector.)

INFRASTRUCTURE AND INTERDEPENDENCIES

The four infrastructure sectors being considered here are "critical" insofar as they produce, directly and indirectly, outputs essential to the economic and social well-being of Canadians. Energy and Utilities and ICT also constitute critical inputs to *other* infrastructure sectors. Any damage or disruption to their operations or to the products and services they provide will have serious consequences.

Critical national infrastructure faces a wide range of physical threats, including extreme weather, vandalism, electrical faults, theft of equipment and theft of materials. That vulnerability increases to the extent that it is dependent upon or is connected to other infrastructure, either through physical and geographic relationships or via a cyber dimension.

Dependency describes a relationship in which one product or service is linked to and influenced by another. As an example, *within* the energy sector, oil supply is highly dependent upon electrical supply because refineries, oil pipelines and service station pumps need electric power for operation. A dependency can also exist *between* sectors: The availability of road, rail and coastal shipping transportation is critical in moving energy products to consumers. *Interdependencies* exist when producers and suppliers of products and services both within and *between* critical infrastructure sectors become mutually dependent upon one another, albeit to varying and unequal degrees.

The defining feature of a modern, interconnected and knowledge-based society and its economy is their dependence on ICT. The digital infrastructure that connects the ten CNI sectors is both a strategic national asset in its own right and a security priority, because the machinery of government, critical national infrastructure (CNI) and provision of essential services such as water, gas, electricity, communications and banking are all largely ICT-dependent. Such *interdependencies* can have serious commercial and societal consequences if there are disruptions in the availability of products and services such as energy, transport services or communications networks.

The consequential effects cascade not only across sectors but across jurisdictions as well—private/public, provincial, territorial and federal. Effective protection of these vital cyber links is likely to require new defensive and pro-active initiatives spanning technology, education, policy and law. While information and communications technologies are providing enterprises with opportunities, these come at the cost of enhanced vulnerability to the diversity of threats inherent in a globalized world.

Protecting—and preventing failures in—the direct and indirect infrastructure linkages that support critical facilities requires a detailed understanding of organizational functions and operational implications in order to identify how and where internal structures link to external infrastructure. Increasing connectivity enhances the likelihood of unanticipated effects beyond the local level, sometimes known as *the butterfly effect.* The complexity of the links means that achieving a sufficiently comprehensive "situational awareness" is a major challenge, but once identified, new technologies, processes and best practices can help contain, dissipate and mitigate disruptions.

Webs of tightly coupled networks and systems are connected to each other at multiple points through a wide variety of both physical and electronic mechanisms. Complex interdependencies of critical infrastructure through information communication technologies have made key sectors increasingly vulnerable to attacks against these networks.

As an example, data communication systems and computerized methods of automatic command and control (SCADA) are widespread across Canadian critical infrastructures: These Internet-linked SCADA systems enable central monitoring and control over production and delivery processes, whether at particular facilities or at complex interdependent infrastructures spread

throughout wide geographic areas. Spies, terrorists and malevolent hacktivists seek to penetrate these networks in order to obtain information, interfere with services or launch further attacks. The energy, transport and finance sectors are particularly vulnerable to disruptions of this kind, which can have a dramatic impact on other sectors such as health.

Public institutions and commercial enterprises are increasingly using broadband and wireless technologies, whether fixed or mobile, for their telecommunications services: both depend on a steady electric power supply. Although mobile base-stations have a back-up battery source, this typically lasts only for a relatively short time, making them vulnerable to outages in the mains power supply. Moreover, because wireless services connect into the core telecommunications infrastructure, any major problems that affect land-line telephones may well take mobile phones and Wi-Fi hotspots out of service too. Even when this doesn't happen, a sudden shift of traffic can overwhelm mobile phone services as was the case in the immediate aftermath of the 7/7 London bombings in 2005. While the interdependencies among all the various infrastructures can probably never be fully known, increasing connectivity means that the failure of one critical component is likely to have far-reaching, reverberating effects. The various types of failure can be categorized as follows:

a) *Common-cause failure*—various facilities (fuel storage, airports and power stations) that are located in geographic proximity are likely to be harmed by a single incident of flooding;

b) *Cascading failures*—Disruption of a control system in one infrastructure (for example, electric power, water) leading to the disruption of a second infrastructure (such as railway transportation when signals are disrupted), and then a third (for example, a food supply chain), and so on, even if there is no *direct* dependence. A cyber attack could directly affect such cascading failures.

c) *Escalating failure*—Disruption of one infrastructure (a communications network) hampers the effort to fix other infrastructures that have been damaged by other entities (for example, emergency services, commerce).

Recent disruptions to civil aviation, a basic infrastructure in developed societies, illustrates the criticality of physical and geographic relationships to the industry, but any disruption to the proper functioning of the computerized systems for air traffic control would harm all air traffic. The extensive use of SCADA systems

increases vulnerability to cyber attacks in other CI sectors, which will then be subject to the cascading and escalating effects of these disruptions.

The process of identifying interdependencies and associated cyber and physical vulnerabilities requires stakeholders to work together collectively in order to apply appropriate strategies to reduce risk where possible; close gaps in preparedness; and achieve resilience by, for example, ensuring a degree of substitutability and planned redundancies. Experts have developed and are employing tools to address the complexities of interdependent national infrastructures, including process-based systems, dynamics models, mathematical network optimization models, physics-based models of existing infrastructures, and high-fidelity agent-based simulations of systems.

Many private sector/owner operators are not adequately aware of existing interdependencies that could impact both the service providers on which they depend and their own ability to continue operations and services to their clients. Their vulnerability to the cascading effects of an ICT failure in another element of their operational chain makes it difficult for stakeholders to undertake the fundamental task of risk management: prioritizing cyber-related risks in order to identify those that can be tolerated, those that can be avoided or displaced in advance, and those that absolutely require mitigation responses. Owner/operators who are adequately aware cannot by themselves reduce the risk, since interdependencies require a collaborative private/public sector approach.

CHAPTER 2
THE CYBER-THREAT ENVIRONMENT

It is useful to distinguish those actions carried out for political or ideological purposes, which are deliberate actions to alter, disrupt, deny, deceive, degrade or destroy computer systems and services, i.e. to render them unavailable or unreliable, from those that are perpetrated for intelligence-gathering purposes. These threats emanate from international terrorism (which may be encouraged and assisted by foreign interference or state entities), state-sponsored espionage and sabotage, and malevolent hacktivism—any of which may utilize someone inside the organization to carry out or assist in the attack. Insider threats are those posed by personnel who have been suborned or "emplaced" within organizations for hostile purposes. Rarely is open-source information available on manifest insider threats, since organizations tend to be reticent about any such matters for reputational reasons.

The WikiLeaks affair of 2010, allegedly the product of an insider leak, exposed thousands of U.S. diplomatic cables and prompted questions about the value and vulnerability of politically sensitive computerized information resources. This and other cyber attacks on computer systems have resulted in government documents being accessed and the private information of individuals and businesses being exposed and compromised. Such exploitations are most effective when the target remains unaware that a compromise of data has occurred and the normal functioning of the system remains undisturbed.

It is an attribute of ICT that its widespread availability, coupled with near-ubiquitous competencies in computer technology, enable cyber attacks to be mounted by a broad spectrum of potential perpetrators. These could encompass formal organizations, loosely structured groups or even individuals. Motivations could range from legitimate protest to espionage or the promotion of extremism. At the highly organized end of the spectrum, the Chinese People's Liberation Army is reported to have deployed a dedicated signals intelligence unit for cyber-espionage; at the more loosely-structured end of the spectrum are located anarchist groups, anti-globalization activists and malicious hacktivists like Anonymous, which eschew a hierarchical structure and operate in an iterative, consensual communitarian mode. Straddling these two extremes are al-Qaeda and its affiliates, who are organized around a strategic leadership, albeit with a widely distributed global operational network, including operatives well-qualified in computer engineering.

The analysis that follows identifies the vulnerabilities and examines the declared intentions, strategies, objectives and demonstrated capabilities of those entities known to have threatened Canada's CNI, including government information systems. These threats include:

- International terrorism, most notably al Qaeda and its auxiliaries
- State-sponsored terrorism, espionage and sabotage
- Malicious hacktivism
- Insider threats

While the many instances cited below are categorized under one of these headings, it should be apparent that the cyber dimension has blurred the lines between them: In the early stages of an attack, it may be impossible to specify whether an actor is state-sponsored, autonomous or part of a malicious or criminal group. The coincidence and complexity of motivation and means makes attribution, i.e. tracing the event to the originating entity, a difficult and lengthy process that may never be satisfactorily accomplished.

INTERNATIONAL TERRORISM

Canada's new Counter-Terrorism Strategy, identified "violence driven by Sunni Islamist extremism" as "the leading threat to Canada's National Security."[11] According to the Strategy:

> Al-Qaida, led by Ayman al Zawahiri since the death of Usama bin Laden in May 2011, remains at the forefront of Sunni Islamist extremism and continues to serve as an ideology and inspiration for potential terrorists worldwide. Although al Qaida capacities have been constrained in recent years by global counter-terrorism efforts, other Sunni Islamist groups affiliated with al-Qaida—either through formal allegiances or by looking to al Qaida as an example—have evolved and pose a substantial threat to Canada and the international community.[12]

The Strategy notes that critical infrastructure protection and especially civil aviation have long been targeted for attack by terrorist groups.[13]

Al-Qaeda and its affiliates have demonstrated a remarkable agility in transforming themselves into an elusive, eclectic global network of groups, cells and homegrown auxiliaries capable of mounting deadly attacks on perceived enemies of Islam. In their religious discourse, tactical doctrine and operations, al-Qaeda and its affiliates have explicitly and directly threatened the economic infrastructure of targeted countries, which include Canada. Their so-called economic jihad[14] is intended to "confuse and suffocate (their) economy and threaten (their) economic and political future."[15] Priority targets have included government-owned property, banks, global corporations, and "wealth belonging to disbelievers with known animosity towards Muslims."[16] The strategic objective, in the words of Osama bin Laden, was "bleeding America to the point of bankruptcy."[17]

Energy infrastructure, and in particular petroleum facilities, pipelines and oil tankers, emerged as a primary target of the economic jihad. Attacks on energy infrastructure have been intended to damage and weaken the economies of perceived enemies of Islam, first and foremost the United States, so as to diminish their industrial, financial and military capability to resist the jihadist onslaught. As the largest single exporter of oil and natural gas to the United States, Canada and its energy infrastructure were explicitly threatened. In addition, Canadian oil company interests in Yemen have also been attacked.

Civil aviation has likewise been a prominent target for al-Qaeda terrorism as well as for international terrorists in general, as is noted by Canada's new Counter-Terrorism Strategy.[18] Passenger flights, cargo flights, and airport facilities have all been subject to terror attacks as part of al-Qaeda's proclaimed economic jihad against the West.[19] A 2006 plot, dubbed "Operation Overt" by British police, resulted in the arrest and subsequent conviction and sentencing to life imprisonment of an al-Qaeda-inspired cell for planning suicide bombing attacks on Trans-Atlantic flights destined for North America. Following a thwarted 2010 plot to blow up an air cargo flight over eastern North America, its so-called Operation Hemorrhage, the al-Qaeda operational planner disclosed that their "...objective was not to cause maximum casualties but to cause maximum losses to the American economy."[20]

In a follow-up statement extolling the economic jihad, al-Qaeda ideologue Yahya Ibrahim warned publicly that "[w]e will continue with similar operations... We are laying out for our enemies our plan in advance because as we stated earlier our objective is not maximum kill but to cause a hemorrhage

in the aviation industry, an industry that is so vital for trade and transportation between the U.S. and Europe."[21]

Also in the Transportation sector, passenger railways and urban transit systems in several countries, including Germany, France, Spain, the United Kingdom and the United States, have been targeted by international or homegrown jihadists affiliated with or inspired by al-Qaeda. According to the U.S. Transportation Security Administration, unidentified hackers, reportedly from abroad, launched cyber attacks against an American railway company, disrupting rail signalling and traffic in the northwestern United States for two days in December 2011.

///

Consistent with this concept of economic jihad, Dr. Ayman al-Zawahiri issued a video pronouncement in February 2011 urging jihadist operatives to innovate and find new ways and means of attacking high-value infrastructure targets: "If we are not able to produce weapons equal to the weapons of the Crusader West, we can sabotage their complex economic and industrial systems and drain their powers... Therefore, the mujahideen [Islamic warriors] must invent new ways, ways that never dawned on the minds of the West."[22]

The first recorded incident of a relatively successful large-scale terrorist cyber attack on corporate computer systems was attributed to the Tariq bin Ziyad Brigades for Electronic Jihad and took place in 2010. While no evidence is yet available of systematic cyber-terrorism on the part of al-Qaeda or its affiliates, the updated UK counter-terrorism strategy ['CONTEST 2'] introduced in July 2011 warned that following the death of Usama bin Laden, al-Qaeda has called explicitly for cyber jihad along with other terror operations.[23]

Commenting on the IT capabilities of Islamist terrorist groups, U.S. officials have admitted that they underestimated the time al-Qaeda had spent mapping vulnerabilities. American authorities reportedly detected operatives using telecom switches in several countries, including Saudi Arabia and Pakistan, to explore digital systems that control U.S. nuclear power plants, emergency telephone services, and water storage and distribution. A computer seized from

an al-Qaeda safe-house in Kabul contained an engineering program used to locate stress weaknesses in buildings, bridges and dams.

Certain Islamic scholars have recently underlined their support for the new phenomenon of "electronic jihad," arguing that "any attempt to 'spite the enemy' and endorse religion is legitimate."[24] They consider that Muslim youth involved in this phenomenon are in fact leading a jihad.

Al-Qaeda and its affiliates and homegrown auxiliaries have long demonstrated their cyber capabilities in utilizing ICT for their purposes. In a special report prepared for the United States Institute of Peace, Professor Gabriel Weimann identified eight ways in which contemporary jihadist militants have exploited the capabilities of the Internet, notably for psychological warfare, propaganda and publicity, data mining, fund-raising, recruitment and mobilization, group networking, sharing information, and for planning and coordinating actual attacks.[25] It is noteworthy that al-Qaeda recruitment seems to have produced a very strong contingent of university graduates in computer science and information technology among its ranks. A University of Oxford study of Islamic radicals indicates that computer engineers are highly over-represented among members of militant jihadist groups in jurisdictions across the world.[26]

It seems clear that al-Qaeda and its affiliates have access to the skills and capabilities needed to mount a cyber effort in support of its declared economic jihad targeting critical infrastructures in the 'Crusader West,' including Canada. The likelihood that terrorists might use cyber attacks against their declared enemies is enough in itself to raise security costs, especially in the case of al-Qaeda, as it has declared "an economic and electronic jihad" to weaken the economies of the USA and its allies. Thus, critical infrastructure might be targeted both as an end in itself and as part of a broader strategic objective. There is little doubt that terrorist organizations are a threat to computer networks, but that threat is enhanced to the extent that they are able to attract state sponsorship.

STATE-SPONSORED TERRORISM, ESPIONAGE AND SABOTAGE

State-sponsored terrorism

While Iran and, to a lesser extent, Syria remain the most active state sponsors of terrorism, many other states will be unable to prevent territory or resources from being exploited by terrorists. In Lebanon, Hizbullah maintains training camps, engages in weapons smuggling and drug trafficking, and stocks thousands of rockets for attacks against Israel.

In January 2012, the Palestinian Hamas called for an escalation of Internet hacking against Israel. Hamas spokesman Sami Abu Zuhri said in a statement e-mailed to reporters in the Gaza strip, "Penetrating Israeli websites means opening a new field of resistance and the beginning of an electronic war against Israeli occupation."

Israeli Prime Minister Benjamin Netanyahu established a National Cyber Directorate in August 2011 to guard against infiltration of the country's government and business computer systems, but in early 2012 hackers identifying themselves as "group-xp, [the] largest Wahhabi hacker group in Saudi Arabia," obtained and posted the details of thousands of Israeli credit card holders (January 2012) in a bid to harm their ostensible "enemy" personally and financially.

Cyber attacks are a perfect asymmetric weapon: unlike physical attacks, they are relatively cheap and it is often difficult, if not impossible, to identify those responsible, yet they can wreak enormous economic and collateral damage. According to a new U.S. strategy document, China and Iran are leading the pursuit of low-cost "asymmetric means," like cyber attacks, to counter American military force. The aim is not to defeat, but to slow down or distance the adversary. The strategy document cautions that these relatively inexpensive measures are spreading to terrorist and guerrilla cells.

Although extremists and terrorist cells often comprise individuals with high-level skills in engineering and computer sciences who have the cyber capabilities to launch their own attacks, they might also be willing to act as proxies for states whose strategic objectives coincide with or are deemed to further their own. The most serious threats to critical infrastructure—Advanced Persistent Threats (APTs), including highly sophisticated worms and viruses such as Stuxnet and Duque—are associated with states because of the level of technical and financial resources required to develop them. The risk is not only that they will

be used to gain unauthorized access in order to control the software governing the functioning of the infrastructure, but also that a malicious package will be inserted for purposes of espionage or sabotage.

While most of the publicly known cyber attacks are perpetrated by hacker enclaves or hacktivists, security authorities have long known that foreign nations and organized crime have daily been stealing gigabits of data. These sophisticated and well-resourced actors do not publicize their actions because, unlike hacktivists, they deem it is not in their interest to do so.

State-sponsored espionage and sabotage

Counter-terrorism is the current priority, but other threats are causing growing concern: As is the case with other countries in the Western world, but particularly the USA, Canada's dependence on digital networks and Internet-based communications has increased its vulnerability to cyber attacks, a large proportion of which have been reportedly attributed to government-backed hackers from China and Russia.

Just as the incidence of *corporate* espionage or illicit activities to gain access to proprietary information or technology for commercial advantage has been on the rise, so too has state-sponsored *economic* or *political* espionage that can be defined as illegal, clandestine or coercive activity by a foreign government or its agents for global strategic purposes. The demarcation line between the two is often a fine one, especially where state-owned foreign enterprises are involved.

///

Espionage activities against Canada are being conducted at levels equal to, or greater than, those witnessed during the Cold War. Cyber attacks launched over the Internet are the fastest-growing form of espionage. Canada's open society, strong international relationships and advanced industries such as telecommunications, mining, agriculture, biotechnology and the aerospace industry make it an attractive target.

In addition to rendering government and critical national infrastructure services unavailable or untrustworthy,[27] espionage or foreign interference activities can harm Canadian interests through the theft of confidential strategic government, political and military information or applications; the loss of assets and leading-edge technologies; the theft of intellectual property and commercial or weapons-related information; corporate acquisitions that pose potential risks to strategic national critical infrastructure; and the illegal transfer of dual-use technologies. **For example,** Canadian government departmental systems and networks came under direct and indirect attack in January 2011 by rogue hackers, reportedly Chinese, who gained access through malicious, targeted emails disguised as legitimate messages.

Such intelligence-gathering operations are difficult to detect because they are not intended to disturb the normal functioning of computing systems or alert users to the compromise. Stopping the theft of intellectual property through cyber espionage has become a key U.S. cyber strategy objective.[28]

The tools and techniques used in cyber attacks are in a constant state of development and incorporate new computer-related technologies and Internet-related capabilities. Massive *Distributed Denial of Service* (DDoS) attacks, such as those perpetrated against Estonia in 2007 and Georgia the following year, involved robotic networks ("botnets") commanding countless infected computers to simultaneously overwhelm target systems with malicious inputs. Government websites, Internet traffic, banking, media and mobile phones were all affected. The scale of these attacks pointed to the involvement of Russia, but DDoS attacks are also launched by criminal networks operating for profit and hacktivists seeking to obtain sensitive information or embarrass government authorities.

A worldwide attack in 2009 referred to as the "Ghostnet" episode was uncovered by the Information Warfare Monitor, a leading Canadian cyber facility. In that attack, which infected more than a 1000 computers in various countries, the networks of several governments were compromised, with presumably a loss of state and commercial secrets.

In another cyber event in 2010, 15% of American Internet traffic over a relatively brief period was mysteriously re-routed through China before reaching its intended recipients. Large corporations, the Pentagon and law firms in the USA, Britain and Canada are among those said to have suffered data breaches

in recent years, many reportedly linked to computers in China. Hackers based in China allegedly targeted law firms as part of an effort to derail the takeover bid by BHP Billiton Ltd. for Potash Corporation of Saskatchewan, thereby promoting China's own interests in acquiring natural resources. Widespread attacks in August 2011 (dubbed "Operation Shady RAT" [random access tool]), reportedly state-sponsored by China, targeted 72 organizations around the world, including the United Nations, governments, companies and the Government of Canada.

Although commercial espionage against global corporate entities such as Google, Sony and Lockheed Martin can have strategic consequences, Advanced Persistent Threats (APTs), which have recently been targeting government, corporate and control networks with sophisticated viruses and "cyber worms," are a source of major concern. These appear to be aimed at the navigation and mapping of information and control systems upon which the integrity and availability of critical national infrastructure such as electric grids, nuclear power stations or financial networks depend. By infecting control systems, they can not only provide the means to copy or steal information about design and operating technologies, but also be programmed to damage or destroy the infrastructure at some future date, perhaps in a time of crisis or war.

The resources necessary to develop these sophisticated viruses and worms point either to direct state involvement or to state sponsorship of proxies such as criminals, terrorists or hackers. There is a growing tendency for states to use non-state actors as cut-outs to disguise their own involvement. China and Russia have powerful cyber capabilities as do Iran, North Korea and even Myanmar[29] but such attacks are deniable because proving attribution is difficult. Non-state actors are likely to be well aware of the value of cyber weapons like these, but while they may not have the organic capability to mount an attack on their own, they may be available "for hire."

While no immediate damage or disruptions have so far been caused, the dormant software left behind can be programmed to control, disrupt or destroy elements of the targeted system at a time of the attacker's choosing. This is clearly a national security threat and one that is a source of major concern given the cyber security deficiencies identified by regulatory bodies and associations of critical infrastructure owner/operators.

Such attacks are akin to strategic cyber weapons—a game changer that is being described as comparable to the advent of nuclear weapons. While there are significant differences between nuclear and cyber attacks, both can have catastrophic consequences. Moreover digital weapons are cheaper and instantaneous, provide virtually no warning, and are low-risk. They can lay dormant in a victim's networks for sometime after being routed there through two or more intermediate nations. This possibility gives the attacker clear advantages over the defender.

In January 2012, the U.S. government expelled the Venezuelan consul-general in Miami, Florida, for allegedly conspiring with Iran to mount cyber attacks on American nuclear power plants. The plan was presumably a reaction to Iran's fears of a future assault on its nuclear program. The government of Venezuela's response to the expulsion was to appoint the former consul-general to the position of Minister of Defence. In January 2012, Azerbaijani authorities arrested suspected Iranian agents for plotting attacks on prominent foreigners, including Israel's ambassador and a local rabbi, after they hacked into state websites to make threats and post anti-Israel messages.

The cyber dimension has changed the character of espionage, which once bore a clear hallmark and was practiced by intelligence professionals. Now, although ideological, political and economic motivations may be similar, non-state actors have entered the arena and cyber cut-outs and technologies make detection and attribution more difficult. The espionage objective of gaining strategic advantage by stealing secrets to identify the adversary's capabilities, strengths and weaknesses can now be achieved through actors and means that are deniable and considerably more diverse and ephemeral. The same modus operandi can be used by opportunistic criminals, corporate competitors or foreign nation states, so that attempting to identify the intent, targets and actors may be an elusive exercise, at least in the early stages.

MALICIOUS HACKTIVISM

Hacking is a growing phenomenon. Whereas most incidents of hacking into computers or computer networking seem to be motivated by criminality, protest or the technical challenge *ipso facto*, malicious hacking by activists or hacktivists who target critical infrastructure assets could constitute a distinct threat to national security.[30] Canadian and international oil companies have warned that

the increasingly frequent and carefully targeted cyber attacks on their computer-controlled operating and information systems by hackers, mostly motivated by criminal or commercial interests, could wreak global havoc through oil supply disruptions. Hackers may operate individually or as part of more-or-less informally structured groups sharing a libertarian/communitarian philosophy.

Last year, an international hacking group known as "Anonymous" succeeded in temporarily disabling online payment sites of credit card companies and PayPal for refusing to transfer donations to the WikiLeaks organization. Later in the year, the same hacktivist group briefly took down the New York Stock Exchange website in support of the Occupy Wall Street demonstrations. Then in late December 2011, Anonymous issued a formal warning that it would black out the entire Internet should the United States dare to enact the Stop Online Piracy Act. Recently Anonymous expressed an intention to target industrial control systems of oil and gas companies as part of its "green" energy agenda, which specifically supports the environmentalist campaign against the Alberta oil sands and the proposed Keystone XL oil pipeline.

Elements within certain of Canada's domestic single-interest groups have demonstrated a propensity to target critical infrastructures for violent direct action as part of their protest agenda. Among the most active of these radical elements are those claiming to represent anarchist, anti-globalization, or environmental causes. Since most of these protest campaigns aim to capture public attention, and thus seek visibility, these groups seem to be less predisposed to resort to surreptitious techniques like cyber attacks in the current context.

In November 2011, a global critical infrastructure protection survey prepared by the Symantec Corporation provided details of a series of attacks launched against some forty-eight Fortune 100 companies involved in the industrial chemical production sector. The "Nitro Attacks," as they were dubbed, were traced to a virtual private server (VPS) in the United States but researchers eventually discovered the system was owned by a "20-something male" located in China's Hebei province.

The U.S. National Cyber Security and Communications Integration Center estimates that Anonymous and other malicious hackers "could be able to develop the capabilities to gain access and trespass on [industrial control system] networks very quickly."[31] Whereas in some cases there is reportedly strong evidence that foreign states are behind the compromise of SCADA systems,

other incidents appear to be the work of hackers whose purpose is to flaunt the cyber skills that have given them control over key services.

Some recent incidents of malicious hacking into critical infrastructures in 2011 and 2012 include:

- Municipal infrastructures in three U.S. cities were compromised during 2011, in what was recently described by Michael Welch, Deputy Assistant Director of the FBI's cyber division, as "an ego trip for a hacker who had control of a major city's critical systems."

- The hacking into the Stratfor intelligence and international affairs analysis by the AntiSec faction of Anonymous in December 2011, which reportedly released personal account information about some 850,000 individual subscribers, who allegedly included Canadian security officials, British intelligence, military and police personnel and NATO staff.

- An attack on an American railway company's computers by suspected foreign hacktivists in December 2011 disrupted railway signals, thereby interfering with rail traffic around the northwestern United States, according to the Transportation Security Administration.

- In February 2012, hacktivists associated with Anonymous intercepted a nominally secure telephone conversation between the FBI and Scotland Yard, which was being transmitted by Internet, and which discussed a joint inquiry into cybercrime. This conversation was published by Anonymous on their website. On the same day, Anonymous also temporarily took down the website home page of the DHS.

- In mid-February 2012, Anonymous announced that it had successfully taken down the U.S. Central Intelligence Agency website, as well as the websites of the State of Alabama and Mexican Chamber of Mines.

Once hacktivists identify a target they usually seem to be able to compromise the integrity of its cyber or information technology systems. Indications are that public figures, governments and industry groups are likely to be targeted for political or ideological reasons and have their cyber systems disrupted, as was the case in the Stratfor hacking incident. More commonly, malicious hackers have engaged in "phishing" expeditions and other deception operations, which are devised to extract personal details about individuals or important proprietary business information from specific organizations for purposes of identity theft and illegal access to sensitive cyber systems.

Hacktivists and their fellow cyber warriors are constantly devising new techniques for cracking into targeted systems. Several months ago Anonymous announced that they had replicated the code for the notorious Stuxnet virus, which was distributed over the Internet. And while Distributed Denial of Service (DDoS) attacks such as those carried out by Anonymous in 2011 are gaining popularity, there are indications that in 2012 they will become even more sophisticated and effective, as attackers shift from the network level to the applications and business levels. For example, the #RefRef tool which was introduced in September 2011, exploits SQL injection vulnerabilities used to perform DDoS attacks.

According to McAfee Inc., more organized digital disruptions by malicious hacktivists are likely to occur in 2012 because many industrial and national infrastructure networks are not designed for modern connectivity and are therefore especially vulnerable: "We expect attackers to take advantage of the situation in 2012, if only for blackmail or extortion, but in a worst-case scenario public utilities such as water and electrical services could be disrupted." [32] In January 2012, McAfee itself was reported to have been penetrated by hacktivists associated with Anonymous.

The DHS has reported a rapid rise in the number of private organizations requesting the Department's assistance to protect their automated control systems. Yet, even sophisticated organizations can sometimes fail to realize they have fallen victim to hackers, and are likely to remain reticent about

acknowledging any compromise of data for reputational reasons. General Keith Alexander, Director of the National Security Agency (NSA), recently compared current business defences to the Maginot Line, the French fortifications built after World War I that failed to halt the German advance in World War II. "We put up a defensive perimeter and then we wait." He indicated that rather than waiting, "companies and Internet providers should be actively scanning for 'signatures' that might indicate new types of attacks, and should then share these with others who could be affected."[33]

INSIDER THREATS

The insider threat refers to any attack perpetrated or assisted by a member of the staff or workforce of a company, critical infrastructure organization, or government department or agency. Disaffected or suborned staff members, or those outsiders who are infiltrated into the organization for the specific purpose of carrying out an attack against it or providing information for others to do so, constitute a serious and growing threat. Infiltrators are members of a group or agents of a hostile foreign intelligence organization who are selected because their skills, motivation and ability enable them to live a cover identity that earns them access to employment and sensitive information and to areas within a particular target organization.

Insider threats may arise among disgruntled or embittered staff through financial seduction, as a demonstration of religious zeal, or because of strong disagreement with government policies. An important factor prompting insider betrayal has been the trend towards organizational restructuring, such as downsizing, outsourcing, displacement of regular employees by part-timers, and even rapid technological change. Insider betrayal may also be motivated by a strong attachment to a foreign identity.[34]

Apart from disgruntled *bona fide* employees, the insider threat arises from agents or moles planted inside sensitive organizations that are being targeted by adversaries. Al-Qaeda's strategic doctrine and operational tactics approve the recruitment and emplacement of operatives into positions within key infrastructure sectors in targeted countries.[35] Particular emphasis is placed on infiltrating police services, armed forces, political parties, the media, Islamic groups, petroleum companies, private security firms and sensitive civil institutions. Recent research findings indicate that those infiltrated in this

way could pose a potentially greater threat than disgruntled employees.[33] An adversary operating from within represents an especially difficult threat to detect and withstand because of the sensitivities involved in the surveillance of one's own workforce and the natural apathy or reluctance of fellow workers to report irregular or suspicious behaviour.

A report issued by the DHS in July 2011, entitled *Insider Threat to Utilities*, has warned that "violent extremists have, in fact, obtained insider positions" in American energy utilities and present a "significant" physical and cyber threat to critical infrastructure.[37] The report further noted that "insider information on sites, infrastructure, networks and personnel is valuable to our adversaries and may increase the impact of any attack on the utilities infrastructure." Insiders have also been recruited by foreign states, notably China, to conduct economic espionage on high-tech manufacturing and resource industries.

Paradoxically, the threat to national security has been increased by new cyber technologies that have made possible the aggregation, storage and rapid retrieval of data. This has made it easier for insiders to perpetrate acts of industrial and economic sabotage against government services and critical infrastructure, as well as creating significant new opportunities. Massive amounts of valuable data can be downloaded and moved via the Internet or onto miniaturized digital devices that can be "exfiltrated" from the organization undetected. Insiders might be able to gain privileged access to cyber systems that scan, monitor and control infrastructure, or they may be able to gather intelligence revealing the cyber and physical weaknesses of plants through unguarded discussions and overheard conversations. Knowledge of the business and its systems gives the insider the advantage of being able to make sense of data that would be opaque to an errant visitor or an opportunistic intruder who fortuitously managed to penetrate the physical security barriers.

Infrastructure sectors and institutions in various jurisdictions that are known to have experienced insider threats from international jihadist elements in recent years include airports, airlines, energy utilities, nuclear plants, petroleum companies, university laboratories, water systems, sensitive government departments and security agencies in Denmark, the Netherlands, the U.K. and the U.S. There are particular concerns about the increasing threats to airports (as distinct from airlines as such) arising from detected instances in various jurisdictions where disaffected employees in duty-free shops and cargo facilities, ground personnel, baggage handlers, and fuel suppliers have been suborned by terrorists.

In Australia, an aggrieved water treatment plant employee sabotaged a computerized control system, causing more than 200,000 gallons of sewage to be released into parks, rivers and the grounds of the Hyatt hotel.[38] In another insider case, a former security guard at a Dallas hospital was recently convicted of corrupting industrial control systems in order to shut down the air conditioning systems at his former workplace. He was sentenced to 110 months in prison in March 2011.

CHAPTER 3
RISKS AND PROBABILITIES OF CYBER ATTACKS

THE CYBER DOMAIN: CHARACTERISTICS AND CONCERNS

Countering cyber threats entails particular challenges because certain characteristics of the cyber domain that are absent or less significant in other domains increase the complexity of assessing the probabilities and risks of cyber attacks.

The pace of change

Cyberspace is a technology-driven domain where game-changing innovations can emerge within days. As such, security threats can arise and evolve so rapidly that the balance of advantage may not swing back and forth as it traditionally does in the action/response cycles of other domains. The cyber-security firm McAfee reports that 60,000 new malware variants are launched virtually every day.

Geographic boundaries

Critical infrastructures tend to be those that operate in global markets and accordingly, international connectivity is indispensable to their business interests. Since there are no geographic boundaries in cyberspace, individuals, groups, and/or nation-state attackers can reside anywhere; their objectives are similarly boundless. The cyber domain, more than any other, has blurred the distinction between domestic and foreign threats, prioritized the requirement to increase international security intelligence gathering, and underlined the need to forge closer working relationships with private sector and foreign partners. Cyber technologies put pressure on the boundaries between organizations, encouraging them to share data more freely, implement the same processes, and converge on the same technologies.

Anonymity and attribution

While cyber threats can usually be analyzed in terms of ends, ways and means, the motive behind a large-scale attack, the technique used and the identity of the cyber-aggressor may be difficult, if not impossible, to determine because

of anonymity and the speed at which cyber threats evolve. The initiative therefore lies with the aggressor to a greater extent than in the case of threats in other domains, especially when the adversary is agile and innovative and the victim remains unaware or slow to grasp the complexities of the cyber threat environment.

Laws, regulations and jurisdictional authority

Protecting critical infrastructure in the ever-changing ICT environment is a demanding proposition, which requires that legislation be kept current with developments. The processes of achieving effective legal regulation or applying political constraints and deterrents are more difficult in the cyber domain than in any other because of the problem of attribution, the speed of evolving new cyber threats and the lack of boundaries.

National and international legislators, law enforcement and regulators are struggling to catch up with emerging cyber threats: rules, protocols and standards are few, disconnected, and often conflicting. These concerns are reflected in the title of a recent report issued by the Security & Defence Agenda (SDA) think-tank, "Cyber Security: The Vexed Question of Global Rules," which, among other recommendations, emphasizes the need to develop best-practice-led international security standards.[39]

State responses tend to be unwieldy and fragmented because jurisdictional issues hamper a cohesive, holistic approach to cyber activities nationally or worldwide. There is no agreed definition of what constitutes a cyber attack on a nation or a breach of sovereignty. At a global level, the fragmented ownership and regulatory control of ICT infrastructure is one of the major challenges. While one country may enact and enforce strict regulatory conditions against cyber criminals, those same criminals may be able to operate relatively openly in other countries that have less-developed programs.

Private sector owners and operators of the vital networks that serve critical infrastructure such as utilities, air traffic control systems, banks and water suppliers, are increasingly looking to the security and intelligence agencies to coordinate alerts, provide threat intelligence, and issue guidance on protecting themselves against the growing number of viruses, worms and other malware being launched. Attempts to meet this need are likely to come up against constitutional, legal, jurisdictional and resource constraints as well as source protection and liability issues. Both sides have reasons to withhold information,

but the potential threat necessitates change. Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector, McAfee has said, "Until we can pool our data and equip our people and machines with intelligence, we are playing chess with only half the pieces."[40]

In the United States, the very law that established the country's intelligence services now prevents them from sharing classified information with private sector businesses. However, the Cyber Intelligence Sharing and Protection Act of 2011 is one of several U.S. initiatives designed to address cyber security in the private sector. The U.S. House Homeland Security Subcommittee has proposed a bill that would require DHS to develop cyber security standards and work with industry to enforce them.

Ethical dimensions

The difficulties often involved in identifying the cyber aggressor or being able to analyze attacks in terms of motives and techniques have implications for threat and risk assessments as well as the ethics governing the security response. A cyber attack may appear to be less dramatic than a physical attack and not immediately viewed in life-threatening terms, but this would be a misleading perception in the case of a major attack on a power grid or the diversion of water systems, both of which could cause deaths and considerable human suffering.

Finding a common framework of ethics, norms and values that can be applied to both aggressors and defenders engaged in cyber "conflict" will be difficult. Attackers may consider implanted software allowing them to disable or degrade the material and service supply chains of potential adversaries in the event of conflict as a preventive and *defensive* action. The defenders, however, are likely to view such an action as *offensive* and a signal of future malign intentions. After jihadist elements had repeatedly launched cyber offensives against its websites, Israel recently said that it would respond to cyber attacks in the same way it responds to terrorist acts.

We do not yet fully understand how social norms are shaped in the virtual world and this affects our ability to deter and incentivize the various actors. It will be difficult to determine and define the acceptable rules of engagement for state, corporate and industrial espionage, especially where the line between private and public enterprise is blurred, or to decide to what extent hacktivist movements should be accommodated as a digital expression of legitimate civil disobedience. Defining the challenges and finding solutions requires an understanding of

human motives. Such an understanding can only be acquired through further research and discussion.

Opposition to initiatives aimed at enhancing cyber security is usually rooted in concerns and expectations about the balance between security and privacy. The way forward would seem to require greater efforts at improving attribution capabilities so as to facilitate and justify actions against cyber attackers, while selectively reducing anonymity without sacrificing privacy rights.

EMERGENT THREATS

For adversaries confronting a stronger opponent in an asymmetric environment, cyberspace provides a relatively low-cost, risk-free haven for a broad range of disruptive, destructive and intelligence-gathering operations. Minor players can exercise considerable power in the cyber domain, which has become a multi-dimensional attack space that enables perpetrators to target critical infrastructures remotely and without physical exposure to defensive forces. Traditional physical methods of protecting critical infrastructure are no longer sufficient, and Canada cannot continue to abide by the kind of reactive, defensive stance that has long characterized protective security.

Offensive techniques and technologies have rapidly evolved over the past twenty years, giving rise to new and more sophisticated threats based on the improvement of attackers' skill sets and the advanced technology at their disposal. Computerized critical infrastructure is not only highly vulnerable to penetration and exploitation via communications networks, but also to the infection of command and control systems, which would render them susceptible to physical destruction. The discovery of the Stuxnet cyber worm virus in 2010, the first that was found to be specifically designed to subvert the process controls of industrial systems, provided evidence of this. This was a new and destructive cyber weapon created to cross from the digital realm to the physical world in a direct attack that required no Internet link and had the potential to damage governments, organizations and critical infrastructure around the world.

Whereas control systems traditionally used combinations of radio and direct serial or modem connections, the current trend towards Internet-linked connectivity between multiple SCADA systems and central office networks has

increased this vulnerability and the risk of cascading consequences across critical infrastructure sectors. The Netherlands Office of the National Coordinator for Counterterrorism has forewarned that there exists "a real possibility" that Stuxnet-type malware will be replicated by adversaries for cyber attacks on vulnerable critical infrastructure systems.[41]

Moreover, the increasing complexity of IT systems also means that there are more exploitable vulnerabilities that arise by accident and more opportunities to hide deliberately introduced vulnerabilities. At the same time, it is becoming harder for the finite number of trusted experts to check systems for integrity. While the SDA report on cyber security highlights the need to address the shortage of skilled cyber-security personnel to counter cyber threats, an Intelligence and National Security Alliance report emphasizes that cyber attackers do not need to be well-resourced or educated.

Furthermore, many Western nations are outsourcing the design, implementation and maintenance of Information Technology across all sectors to third-party providers, including developing countries. While this outsourcing and use of off-the-shelf, commercial technologies occurs for economic reasons, there are inherent security risks involved that the market does not take into account.

The same may be said of cloud computing and large data fusion centres. The rapid movement of data that is an aspect of cloud computing and the archiving of massive volumes of data in one location raise further concerns about Internet security in terms of where cloud data is located and the extent to which it is vulnerable to hackers, espionage or accidental disclosure. Google has sited one-third of its cloud computing in Canada. Moving and archiving concentrated volumes of data to sites whose security is largely untested and whose vulnerabilities are still uncertain, could expose sensitive personal, corporate and even governmental information to potential risk, with far-reaching implications for national security.[42]

The Director of the U.S. Federal Bureau of Investigation, testifying before the Senate Select Committee on Intelligence in January 2012, asserted that threats from cyber-espionage, computer crime, and attacks on critical infrastructure will surpass terrorism as the number one threat facing the United States. If so, this escalating cyber threat will likely have a parallel impact on Canada.

(See Appendix A, which provides more detail on the ICT Sector.)

ASSESSING RISK AND VULNERABILITIES

Conducting assessments of threats and risks is a complex process. The structural complexity of the threat needs to be fully understood and factored into assessments, but this is especially challenging with respect to terrorist threats and the malicious cyber targeting of critical national infrastructure. Private sector vendors of security products have commercial interests to promote that take no account of public sector needs and strategy, while corporate and commercial victims of cybercrime are reluctant to reveal that their networks have been compromised (even supposing they know). These informational impediments to a realistic assessment of threats and vulnerabilities are further exacerbated by the issue of security costs, which we address next.

A reliable way of estimating risk is needed to help managers of critical infrastructure decide how much security is needed at their facility. Risks are usually evaluated on an actuarial basis, which takes into account the record of threats mounted, known vulnerabilities and losses actually incurred. However, many emergent risks are unprecedented and cannot be determined with conventional actuarial methods. These have been described as "wicked risks," because they cannot be assessed actuarially and require an assessment of the probability of the threat materializing. This calls for finely-tuned analytical judgment based on a comprehensive understanding of the prospective player, its organizational complexity, belief system, ideological trends, cognitive and behavioural patterns, tactical doctrine and operational objectives.

In her pioneering work on "wicked risks," Nancy Hayden of the Sandia National Laboratory characterizes terrorism as a complex, dynamically interacting social, technological, and institutional phenomenon.[43] Some of the latest actuarial models developed by U.S. National Laboratories and by specialist risk modeling firms have taken steps to integrate "wicked risk" considerations into their probability assessments. (A number of these models are outlined in Appendix B.)

CHAPTER 4
COUNTERING THE CYBER THREATS: A PARTNERSHIP APPROACH TO CRITICAL INFRASTRUCTURE PROTECTION

Given the rapid changes in information and communication technologies, the Canadian government is not alone in concluding that existing defences will not be enough to ensure the integrity and availability of its information systems nor prevent critical infrastructure from being destroyed or shut down. A mounting sense of growing threats and vulnerabilities has impelled policy-makers in a number of jurisdictions to consider what more can be done to better secure cyber networks, enhance their resilience, and prevent terrorists and others who seek to undermine societal security and competitiveness from attacking critical infrastructures. While the majority of reported cyber incidents are exploitations, which have so far been deemed a lesser threat, U.S. concern about China's strategy of developing its economy by stealing technology is growing and has prompted calls for a more concrete response.

Since the threat derives from the properties of digital technologies, the response to the threat is generally sought among computer experts; if information security is perceived as a technical problem, proposed solutions will focus on identifying the vulnerabilities in an organization's computerized systems and providing engineering solutions—most of which will be identified and implemented through the private market. Technical levels of protection address numerous issues, but the primary means of attempting to build resilience is to invest in back-up, redundancy, air gaps and the like.

While the issue of information security has emerged as a result of technological change, there is growing acceptance that the problem cannot be dealt with solely at a technical-operational level, but rather requires a more holistic approach at a national level. The challenge becomes one of *protecting an information-based society as a whole* rather than protecting information infrastructures. Apart from stimulating investment in defensive technologies, this approach would entail a proactive cyber security initiative on the part of intelligence services to *prevent* infections rather than merely react to them. It would place greater emphasis on combating cyber exploitations that target government and business secrets and are as much of a threat to national security as large cyber attacks that damage or disrupt computer systems. Stopping the theft of intellectual property through cyber espionage is becoming a key objective of U.S. cyber strategy and is likewise a core responsibility of Canada's security and intelligence community.

National security is the prerogative of the *State,* but in Canada it is the owners and operators of critical infrastructure who are considered to be primarily responsible for the security and protection of their own assets. Private sector organizations can insure against actuarial and terrorism risks but, for the most part, senior managements tend to treat security as a troublesome and unwelcome cost of doing business, which must be minimized. Complacency, if not apathy, typically prevails in many executive suites, especially with regard to cyber and terrorist threats, according to an international survey.[44] Security officers rarely have access to their senior management. Indeed, there are known instances where senior executives actually refused to listen to threat assessments from their own security personnel lest they incur liabilities.

A major consideration for owner/operators is the financial cost of ensuring the security of their critical infrastructure assets against cyber threats. This cost burden can include expenses incurred for built-in redundancies, hardware and software solutions, specialist staffing and professional training, as well as contingency planning. While the onus for protection against criminal threats falls clearly on the owner/operators themselves as a cost of doing business, national security-related threats have ramifications that extend beyond the private domain and also affect the public interest.

Accordingly, it would seem appropriate that the costs of protecting critical infrastructure against certain threats to national security be borne in a proportionate manner by all those who benefit: Some assistance from central government revenue to ensure that critical infrastructure owner/operators take account of low-probability but high-consequence risks would better safeguard not only the commercial interests of the owner/operators of critical infrastructure but also benefit the public more broadly and enhance their confidence in government to maintain essential services in times of crisis.

The United States' Cyberspace Strategic Plan aims to improve cyber security resiliency with technology that enables secure software development; to introduce economic incentives like market-based, legal, regulatory, or institutional interventions; and to develop strategies to help security professionals make it more costly and difficult for attackers to act.[45] If enacted next year, a new cyber security bill recently introduced in Congress would designate the DHS as the lead agency responsible for protecting both government and private sector networks, and would require critical infrastructure operators to develop and submit a cyber security plan to the DHS for approval.

A WAY AHEAD—THE ROLE OF INTELLIGENCE

Cyber security is typically perceived as an essentially defensive means of protecting digital assets, with an emphasis on technical solutions. A defensive posture is procedurally passive and reactive and will always trail behind emergent threats. The initiative remains with the adversaries. Consequently, the protection of critical infrastructure and information systems against cyber threats is now rapidly being re-conceptualized as the defence of an information-based society as a whole—a national security consideration. And in national security as in war, the best defence is predicated on a robust offence. In going beyond merely defensive, technical solutions, a proactive approach to the protection of critical infrastructure against cyber threats will have to utilize intelligence capabilities and assets to prevent attacks by identifying and forestalling prospective threats.

Canada's new counter-terrorism strategy incorporates a "deny" element aimed explicitly at reducing potential cyber security vulnerabilities, inter alia, through proactive measures.[46] An assessment of adversaries' current and future cyber capabilities would be an obvious example. Whereas the United States also has a demonstrated ability to conduct cyber attacks to degrade or otherwise destroy an adversary's computerized system, Canada's immediate national security interest lies in mounting an effective, robust campaign against cyber attacks by terrorists and foreign nation-states that denies them the means to operate in this domain.

In the UK, the Centre for the Protection of National Infrastructure (CPNI) works closely with other central agencies to provide advice to businesses and organizations across all sectors of the country's critical national infrastructure, helping mitigate risk and reduce vulnerability to threats in the cyber domain. It also provides warnings, alerts and assistance in resolving serious IT security incidents. The CPNI is a part of the UK Security Service.

Mike McConnell, former Director of U.S. National Intelligence, recently commented on the unique capabilities of U.S. intelligence agencies that could be enlisted to help protect American companies from cyber espionage and attack. The key question is how that capability can be harnessed and made available to the private sector so that critical infrastructure could be better protected.

Although the U.S. is developing more robust and proactive cyber security capabilities, the main priorities, according to McConnell, should be to protect America's critical infrastructure such as the financial sector, the electric power grid and transportation from cyber attack, and to stop the theft of intellectual property through cyber espionage. These mirror Canada's own cyber-security concerns. A new cyber bill approved by the U.S. House of Representatives Intelligence Committee in December 2011 would allow American intelligence agencies to share cyber-threat information with private companies. Since it is the government that has access to intelligence on the threats, but private sector stakeholders who bear primary responsibility for protecting critical assets, some arrangement for dovetailing the two must be found. Very often the owner/operators are actually the first to become aware of new cyber viruses and worms, and therefore it is essential that a formalized process for collecting, analyzing and disseminating information about serious cyber incidents be put in place.

Detection of threats requires, as set out in Canada's new counter-terrorism strategy, "strong intelligence capacity and capabilities, as well as a solid understanding of the strategic drivers of the threat environment, and extensive collaboration and information sharing with domestic and international partners."[47] Canada's security and intelligence community has a unique mandate to act in the interest of national security by virtue of its access to sensitive threat information and its analytic and operational capabilities and experience. Signals intelligence is also key to the detection of immediate threats. Their combined efforts to protect Canadian information networks from intrusions are achieved through a collaborative partnership in which investigative leads are shared in order to assist in the detection, identification and pre-emption of would-be attackers, including insiders.

Along with these core competencies and operational capabilities, Canada's intelligence services has other means to help bring about a more robust and proactive national security response to cyber threats. The information-sharing that already takes place with critical infrastructure stakeholders, as and when appropriate, can be reinforced through the creation of effective partnerships in knowledge capacity-building, which could cement public/private sector collaboration in cyber security. Intelligence services have credibility and a unique competence in performing these roles by virtue of their access to threat information, technical and analytic expertise, and investigative experience.

Critical infrastructure stakeholders in the Energy and Utilities, Finance, ICT, and Transportation sectors in Canada have been accustomed to managing the risks to their facilities at a local level. Nevertheless, it is widely acknowledged by stakeholders in these key sectors that there are weaknesses and gaps in their cyber defences against current threats. A more holistic, finely-tuned partnership approach between the private sector and the security and intelligence community is warranted to help stakeholders—as well as local authorities—offset these vulnerabilities, mitigate any potential damage and pre-plan resilience.

An often-neglected aspect of an intelligence-based approach to critical infrastructure protection, including cyber security, is the training pre-requisite. The recent SDA report on *Cyber Security: The Vexed Question of Global Rules* made the point that a cyber-security skills gap affected the ability of private sector firms to recruit qualified personnel to meet their security needs.[48] Specialized training and qualifications are necessary to prepare corporate security officers for the handling, protection and use of intelligence-based material. Likewise, intelligence analysts and managers must be equipped with the requisite competencies and skills to understand the threats, vulnerabilities and interdependencies associated with specific industrial sectors and processes, as well as their organizational attributes and needs. Without such training and properly qualified security managers and practitioners, no strategy, no tactic and no defence can be fully effective.

A proactive intelligence approach to cyber security for critical infrastructure should demonstrate the following attributes:

- The operational objectives would be to detect and forestall cyber threats to critical national infrastructure and public safety.

- Cyber security activities would be geared to the identification and systematic collection, analysis and reporting of threats to critical infrastructures.

- Intelligence information should be made available on a "need-to-share" basis among partners in the security, intelligence and law-enforcement communities. Private sector owner/operators of critical infrastructure assets would be expected to share their own assessments of vulnerabilities and threats with intelligence services and security authorities, as well as report any compromise of their

networks. This information would be protected on a classified basis.

- Actionable threat intelligence on cyber threats to critical national infrastructure would be disseminated to security-cleared personnel in targeted private sector facilities.

- A rapid reaction capability is required to mitigate attacks, prevent escalation and derive lessons learned in order to advance best practices.

Whether cyber threats arise from international terrorism, state-sponsored espionage or malicious hacktivists, any targeting of critical infrastructure can represent a potential threat to the national security and public safety of Canadians. Intelligence capabilities should be deployed to detect and prevent the targeting of critical infrastructure and ensure the pursuit and prosecution of the perpetrators. A coordinated, intelligence-based response to cyber threats could prevent intrusions into sensitive facilities and ICT systems and mitigate any residual damage.

Intelligence is a key component of tactical and strategic decision-making. In the cyber arena, intelligence can enhance the ability of governments and stakeholders to assess the effects of cyber attacks, mitigate the risks, and streamline cyber security into an efficient and cost-effective process based on well-informed decisions. A 2011 report issued by the Cyber Council of the Intelligence and National Security Alliance (INSA), entitled *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*, began with the proposition that "While quantifiable assessments of the net impact of cyber attacks are difficult to discern, the cost is great enough to warrant the need for a cyber security apparatus supported by sophisticated cyber intelligence."[49] Intelligence support for cyber security within and among critical infrastructure assets should aim to ensure that the cost to adversaries of trying to exploit systemic vulnerabilities is high, that the prospects of success are minimal, that the probable consequential damages are mitigated, and that industry and society are properly prepared for resilience.

APPENDIX A
THE STRUCTURAL DYNAMICS OF THE INFORMATION AND COMMUNICATIONS TECHNOLOGY SECTOR

The Information and Communications Technology infrastructure sector includes telephony, radio and television broadcasting, Internet connectivity, perimeter access controls, and space satellite monitoring and control. In a globally competitive environment, Canadian owner/operators of critical infrastructure facilities, like their counterparts elsewhere, are increasingly likely to introduce sophisticated cyber technologies to promote efficiencies and operational effectiveness.

These new technologies include computerized control systems that are used in many industries to monitor and control sensitive processes and physical functions. They perform vital functions across critical national infrastructure systems including electric power generation, transmission and distribution; oil and gas refining and pipelines; water treatment and distribution; and railways and mass transit systems.

Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. In the electric power industry, control systems can manage and control the generation, transmission and distribution of electric power—for example, by opening and closing circuit breakers and setting thresholds for preventive shut-downs. Employing integrated control systems, the oil and gas industry can control the refining operations at a plant site, remotely monitor the pressure and flow of gap pipelines, and control the flow and pathways of gas transmission. Water utilities can remotely monitor well levels and control the pumps; monitor flows, tank levels, or pressure in storage tanks; monitor water quality characteristics; and control the addition of chemicals. Control systems perform functions that vary from the simple to the complex i.e. monitoring the environmental conditions of a single office, to managing most of the activities in a nuclear power plant.

There are two primary types of control systems: Distributed Control Systems (DCS), which are typically used within a single processing or generating plant, or over a small geographic area; and Supervisory Control and Data Acquisition

(SCADA) systems, which are used for large, geographically dispersed distribution operations. As an example, a utilities company may use a DCS to generate power and a SCADA system to distribute it.

The vulnerability of Internet communications poses significant risks to the critical infrastructure and operations they support. In the past, proprietary hardware, software, and network protocols made it difficult to understand how control systems operated and therefore how to hack into them; today, the drive to reduce costs and improve performance has led organizations to adopt standardized technologies and the common networking protocols used by the Internet. Widely used standardized technologies have commonly known vulnerabilities, rendering more systems susceptible to attacks, while at the same time the availability of sophisticated and effective exploitation tools that are relatively easy to use has increased the number of people with the knowledge to launch attacks. The increased connectivity of these control systems to others, insecure remote cyber connections, and widespread availability of technical information about control systems has escalated the risks and incidence of cyber attacks.

ICT-based technologies are used in the Transportation sector for air passenger reservations and boarding control, air cargo management, and the Free And Secure Trade (FAST) and Pre-Arrival Processing System (PAPS) border pre-clearances for trucking. Internet-linked ICT systems are used in the Finance sector to operate client accounts, remote banking machines (Automated Teller Machines or ATMs), credit/debit card charge card devices, and wire transfers of funds.

SCADA and related ICT technologies are inherently vulnerable to two distinct potential cyber threats: (1) the threat of unauthorized access to control software so as to take over the host infrastructure's functioning; and (2) the threat of malicious packet insertion into the infrastructure hosting the SCADA device for espionage purposes or eventual sabotage. Whereas control systems have traditionally used combinations of radio and direct serial or modem connections, the current trend towards Internet-linked connectivity between multiple SCADA systems and central office networks is creating potential vulnerabilities to cyber attacks—vulnerabilities that may directly lead to the compromise or damage of attendant infrastructure and in addition have a far-reaching impact on society due to interdependencies.

ICT is inherently vulnerable to cyber infiltration, typically via the Internet, for such purposes as accessing and extracting sensitive information, manipulating or diverting data flows, or interfering with SCADA and other industrial control systems. The Internet infrastructure is itself quite robust, with built-in redundancies. There is no evidence of any hostile cyber attack to date (February 2012) actually targeting the Internet.

Critical infrastructure sectors and systems are increasingly relying on space-based Global Positioning Satellites (GPS) for positioning, navigation, and timing (PNT) but while the GPS system is considered to be highly accurate, very robust and reliable, its PNT signals are vulnerable to disruptions due to naturally occurring phenomenon such as space weather events or malicious interference.

Data and the software needed for processing it are increasingly stored in large data centres, installations that make heavy demands on the electricity grid. While these technologies facilitate government and commercial business, they also offer targets of opportunity for criminals and other malicious perpetrators.

Widespread reliance on space-based GPS for positioning, navigation, and timing (PNT) services presents a unique cyber security risk, according to Brandon Wales, Director of the DHS Homeland Infrastructure Threat and Risk Analysis Center. Incidents of GPS interference are reportedly on the increase and include a jamming attempt at Liberty International Airport, Newark, New Jersey in early 2010, when the Ground Based Augmentation System (GBAS), which provides GPS data for aircraft approaches and departures, was targeted.

The rapid movement of data that is an aspect of cloud computing raises further concerns about Internet security, both in terms of where cloud data is located and the extent to which it is vulnerable to hackers, espionage or accidental disclosure. The trend to cloud computing is expected to accelerate so that by 2015 it is expected to account for nearly 34% of traffic at the world's data centers, the huge computing stations that now process and distribute most of the Internet's information. These data centers represent an ever-larger driver of Internet traffic, serving as digital engines for the Internet's most-used services: Google, Facebook, Amazon, Apple's iCloud and many others. Google has sited one-third of its cloud computing in Canada, which can have far-reaching implications for national security. By early 2012, cloud computing systems will also have been developed for disaster management platforms to enable

users (first-responders, governments, relief organizations, volunteers and local residents) to access information, communicate, and collaborate in real-time from all types of computing devices, including mobile handheld devices, such as smart phones, PDAs and iPads.

The ICT sector has been undergoing rapid change: Most organizations rely on the Internet for access to essential business data or software applications—often managed by third party providers. Voice services are migrating online too, with increasing numbers of companies opting for Voice over Internet Protocol (VoIP) as a low-cost alternative to traditional telephony. Unless this is securely designed from the outset, a VoIP channel to and from a network can be a potential security hole in an otherwise secure system.

APPENDIX B
MODELING RISKS AND VULNERABILITIES

Various methodologies have been developed in recent decades by U.S. National Laboratories and private insurers to better evaluate the risks and vulnerabilities of critical infrastructure to terrorist threats and malicious cyber targeting.

In the United States, the DHS has established a National Infrastructure Simulation and Analysis Center (NISAC) to build national knowledge capacity regarding the protection of critical infrastructure. NISAC is charged with providing modeling and simulation capabilities for the analysis of critical infrastructure risks and vulnerabilities, drawing upon research work at the Sandia National Laboratories and Los Alamos National Laboratory.[50]

Sandia Laboratories has developed a methodology to assess risk at various types of facilities and critical infrastructures and to reduce it by a process of identifying and evaluating security system upgrades. Sandia has also collaborated with the Environmental Protection Agency (EPA) and industry groups to develop a risk assessment methodology for assessing the vulnerability of water systems in the U.S. Possible tools include agent-based modeling, cognitive modeling and ideological trend analysis.

The Argonne National Laboratory, in partnership with the DHS, has developed methodology to systematically evaluate the protection posture and vulnerability of critical infrastructures.[51] Sector and sub-sector vulnerabilities are assessed by means of a vulnerability index to identify potential ways to reduce vulnerabilities and assist in preparing sector risk estimates. The owner/operator also receives an analysis of the data collected for a specific asset, which gives an indication of the asset's strengths and weaknesses with regard to security. The initiative is part of a broader DHS Enhanced Critical Infrastructure Protection Program designed to mitigate vulnerabilities, enhance relationships, and improve information-sharing between public and private entities.

AIR Worldwide, a U.S.-based catastrophic risk modeling firm, produced an update of its terrorism model for the United States in October 2011. It is intended for use by insurers and reinsurers to assess potential losses due to terrorist attack. The AIR target/landmark database includes a full spectrum of potential targets at risk from a likely attack, many of which are deemed "trophy

targets." A rigorous assessment methodology is utilized to estimate potential future attacks, taking account of a full range of threats, including those from domestic extremists, foreign regimes and state-sponsored organizations, and loosely affiliated networks of like-minded small groups and individuals.[52]

In the UK, a prominent reinsurance intermediary, Aon Benfield, announced in November 2011 its new "UK terrorism catastrophe model," with updated attack scenarios and probabilities. The model estimates the financial loss to life insurers from potential terrorist events and helps meet the requirements of the proposed European Union Solvency II regulation, which requires insurers to gain a better understanding of their exposures and consequently their reinsurance-buying strategy. This new model simulates attacks against potential UK targets, including places of worship, financial centres, infrastructure, and government and military locations. The model reflects attempts to integrate traditional actual assessments with input on event frequency, credible attack types and damage profiles for various scenarios.[53]

ENDNOTES

(Endnotes)

1 Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats," *Military and Strategic Affairs*, Vol. 3, No. 2, November 2011, p. 2.

2 *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities*, National Research Council Report, p.1. The National Academies Press, 2009.

3 Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (2004), accessible at: http://www.pco-bcp.gc.ca/docs/information/publications/natsec-secnat/natsec-secnat-eng.pdf.

4 Public Safety Canada, *National Strategy for Critical Infrastructure* (2010), accessible at: http://www.publicsafety.gc.ca/prg/ns/ci/ntnl-eng.aspx.

5 Public Safety Canada, *Action Plan for Critical Infrastructure* (2010), accessible at: http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ci-pln-eng.pdf.

6 Public Safety Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (2010), accessible at: http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf.

7 However, there are some private sector and non-governmental organizations that are not deemed Critical National Infrastructure, such as law firms, financial accounting firms, R&D entities and universities, which could be holding information and knowledge resources of national significance, but nevertheless might not be consulted on cyber security under existing partnering arrangements for the Cyber Security Strategy.

8 Public Safety Canada: *Building Resilience Against Terrorism*, (Ottawa, 2012), p. 6.

9 Ibid., p. 22.

10 Ibid.

11 Ibid., p. 7.

12 Ibid.,

13 Ibid., p. 22-23.

14 Al-Qaida in Saudi Arabia: *Excerpts from "The Laws of Targeting Petroleum-Related Interests,"* written by Shaykh Abdullah bin Nasser al-Rashid (aka Abdelaziz bin Rashid al-Anzi), Global Terror Alert, March, 2006 (http://www/globalterroralert.com).

15 Adeeb al-Bassam, "Bin Laden and the Oil Weapon," *Sawt al-Jihad* (Voice of Jihad), Muharram, 28 AH (February, 2007), p. 9. This item appeared as The Knight of Jihadi Media: Issa al-Awshan: "A Special Interview with the Leader: Karim al-Majati - may Allah Accepts Him Bin Laden and the Oil Weapon," *Sawt al-Jihad [Voice of Jihad]*, The Thirtieth Issue, The Month of Muharram, 1428 IC, translated by the SITE Institute, Washington DC: *Al-Qaeda in Saudi Arabia Presents the Return of its Publication, [Voice of Jihad], the Thirtieth Issue.*

16 Sheikh Anwar al-Awlaki, "The Ruling on Dispossessing the disbelievers unbelievers; wealth in Dar al-Harb," *Inspire*, 1431/2010, p. 59.

17 [17] "Full Transcript of bin Laden's Speech," *Al Jazeera.net*, October 30, 2004: http://english.aljazeera.net/NR/exeres/79C6AF22-98FB-4A1C-B21F-2BC36E87F61F.htm.

18 Public Safety Canada: *Building Resilience Against Terrorism*, pp. 22-23.

19 The Head of Foreign Operations, "The Objective of Operation Hemorrhage," *Inspire*, November 1341/2010, Special Issue: Operation Hemorrhage targeting air cargo aircraft, p. 7; Yahya Ibrahim, "$4,200," *Inspire*, November 1341/2010, Special Issue Operation Hemorrhage targeting air cargo aircraft , p. 15.

20 The Head of Foreign Operations, "The Objective of Operation Hemorrhage," *Inspire*, p. 7.

21 Yahya Ibrahim, "$4,200", *Inspire*, p. 15.

22 Association France Presse, "Al-Qaeda calls for the new attacks on West," February 25, 2011, accessible at: http://www.mysinchew.com/node/53796.

23 United Kingdom, Secretary of State for the Home Department: *CONTEST. The United Kingdom's Strategy for Countering Terrorism* (London, July 2011), para. 2.47.

24 Mohammad Atayf, "Scholars speak out in favour of 'electronic Jihad' against the enemy," *al-Arabiya online* at http://english.alarabiya.net/articles/2012/01/29/191307.html.

25 Gabriel Weimann, WWW.Terror.Net. How Modern Terrorism Uses the Internet, United States Institute of Peace Special Report 116 (March 2004).

26 Diego Gambetta & Steffen Hertog, *Engineers of Jihad*, Department of Sociology, University of Oxford, Sociology Working Paper 2007-10m pp. 8, 12.

27 *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities.*

28 Office of the President of the United States: *The Comprehensive National Cybersecurity Initiative* (Washington, 2008), Initiative #3.

29 In 2011 13% of cyber-attacks worldwide were attributed to Myanmar: "Cyber War: Myanmar Leader in Cyber Attacks in 2011, *Asia News*, February 20, 2011, accessible at: http://www.asianews.it/news-en/Cyber-war:-Myanmar-leader-in-attacks-in-2011-22224.html.

30 *Cf.* U.S. Department of Homeland Security, National Cybersecurity and Communications Integration Center bulletin, cited in "DHS warns Anonymous may target critical infrastructure," *Cyber Security News Wire*, November 4, 2011, accessible at: http://www.homelandsecuritynewswire.com/dhs-warns-anonymous-may-target-critical-infrastructure.

31 Cited in "DHS warns Anonymous may target critical infrastructure," *Cyber Security News Wire*, 4 November 2011, accessible at: http://www.homelandsecuritynewswire.com/dhs-warns-anonymous-may-target-critical-infrastructure.

32 Gary Davis, "2012 McAfee Threat Predictions: A look at the latest threats that could affect consumers this coming year," McAfee, December 27, 2011, accessible at: http://blogs.mcafee.com/consumer/2012-mcafee-threat-predictions-consumers.

33 General Keith Alexander, Director of the National Security Agency and Head of Cyber Command, quoted in Jennifer Valentino-DeVries and Julia Angwin, "Defenses against Hackers are like the Maginot Line, says NSA Chief," Wall St. Journal, January 14, 2012.

34 Lisa Kramer & Richards Heuer Jr., "America's Increased Vulnerability to Insider Espionage," *International Journal of Intelligence and CounterIntelligence*, Vol. 20 (2007).

35 Vide. Abu Bakr Naji, *The Management of Savagery* [Trans. William McCants], United States Military Academy, West Point, 2006.

36 Nick Catrantzos, "No Dark Corners: A Different Answer to Insider Threats." *Homeland Security Affairs*, Vol. 6, No. 2 (May 2010).

37 Department of Homeland Security, *Insider Threat to Utilities* (Washington, July 19, 2011), accessible at: http://info.publicintelligence.net/DHS-InsiderThreat.pdf. See also Brian Ross, Rhonda Schwartz & Megan Chuchmach, *New Terror Report Warns of Insider Threat to Utilities*, ABC News, July 10, 2011, accessible at: http://abcnews.go.com/Blotter/terror-alert-warns-insider-threat-infrastructure/story?id=14118119.

38 Symantec's second annual Global Critical Infrastructure Protection [CIP] Survey.

39 Brigid Grauman, *Cyber Security: The Vexed Question of Global Rule. An Independent Report on Cyber Preparedness Around the World* (Brussels: Security and Defence Agenda, 2012). This report was prepared with the support of MacAfee Inc.

40 Ibid., p. 8.

41 The Netherlands, National Coordinator for Counterterrorism, *Technological Developments: Opportunities and Threats for Counterterrorism and Surveillance and Protection Until 2015*, Publication I-8731 (n.d., 2011), p.55.

42 *Cyber Security: The Vexed Question of Global Rule. An Independent Report on Cyber Preparedness Around the World*, p. 58.

43 Nancy Hayden, "The Complexity of Terrorism: Social and Behavioral Understanding Trends for the Future," Information Age Warfare Quarterly, Vol. 1, No. 2 (Summer, 2006); accessible at: http://www.google.ca/search?q=%22Nancy+Hayden%22+%2B+wicked&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a; see also Nancy Hayden, "The Complexity of Terrorism: Social and Behavioral Understanding," in Magnus Ranstorp, ed., *Mapping Terrorism Research. State of the Art, Gaps, and Future Directions* (London: Routledge, 2007).

44 Symantec Corp, 2011 *Symantec Critical Infrastructure Protection Survey* (October 2011), accessible at: http://www.symantec.com/content/en/us/about/media/pdfs/symc_critical_infrastructure_protection_survey_2011.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Oct_worldwide_CIPSurvey.

45 Office of the President of the United States, *Trustworthy Cyberspace: Strategic Plan for the Federal Cyber security Research and Development Program*", (Washington, December, 2011), accessible at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf .

46 Public Safety Canada: *Building Resilience Against Terrorism*, pp. 18-19.

47 Ibid., p. 15.

48 *Cyber Security: A Vexed Question of Global Rule. An Independent Report on Cyber Preparedness Around the World*, pp. 43-44.

49 Intelligence and National Security Alliance (INSA), *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*, September 2011, p 3.

50 NISAC prepares and shares analyses of critical infrastructure and key resources (CIKR), including their interdependencies, vulnerabilities, consequences, and other complexities, under the direction of the Office of Infrastructure Protection (IP), Infrastructure Analysis and Strategy Division (IASD). To ensure consistency with IP priorities, NISAC initiatives and tasking requests are coordinated through the NISAC program office.

51 William Buehring, Ronald Whitfield, Ronald Fisher & Michael Collins, "Protective measures and vulnerability indices for the Enhanced Critical Infrastructure Protection Programme," *International Journal of Critical Infrastructures*, Vol. 7, No.3 (2011), accessible at: http://www.inderscience.com/search/index.php?action=record&rec_id=42976&prevQuery=&ps=10&m=or.

52 Air Worldwide: "Terrorism," accessible at: http://www.air-worldwide.com/terrorism.aspx; "Assessing Terrorism Risk Ten Years After 9/11," accessible at: http://www.air-worldwide.com/PublicationsItem.aspx?id=21161.

53 Aon Benfield Press Release, November 14, 2011: Aon Benfield launches UK terrorism catastrophe model with updated attack scenarios and probabilities, accessible at: http://aon.mediaroom.com/index.php?s=43&item=2481.